

FILED
JAN 31 2019
 Clerk, U.S. District and
 Bankruptcy Courts

UNITED STATES DISTRICT COURT
 FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	:	CRIMINAL NO.
	:	
v.	:	
	:	
BRIAN JAMES LAPRATH,	:	
Defendant.	:	

STATEMENT OF OFFENSE

The parties in this case, the United States of America and the defendant, Brian James LaPrath, stipulate and agree that the following facts are true and accurate. These facts do not constitute all of the facts known to the parties concerning the charged offense; they are being submitted to demonstrate that sufficient facts exist that the defendant committed the offense to which he is pleading guilty, Laundering of Monetary Instruments, in violation of 1956(a)(2)(A).

Statement of Facts

A. The Website

Beginning in September 2017, law enforcement initiated a large scale investigation into a Tor based child pornography website, hereinafter referred to as “The Website.”¹ Tor is a computer network designed to facilitate anonymous communication over the Internet. The Tor network does this by routing a user’s communications through a globally distributed network of relay computers, or proxies, rendering conventional Internet Protocol (“IP”) address-based

¹ The actual name of “The Website” is known to law enforcement. The disclosure of the name of The Website would potentially alert its users to the fact that law enforcement action is being taken against users of The Website, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified herein as “The Website.”

methods of identifying users ineffective. To access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle." When a Tor user accesses a website, only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address, appears on the website's IP address log. Currently, there is no practical method to trace a user's actual IP address back through those Tor relay computers. The Tor Network also makes it possible for users to operate websites, called "hidden services," in a manner that conceals the true IP address of the computer hosting the website.

The Website operated as a hidden service on the Tor network until March of 2018. The Website was used to host and distribute video files depicting child pornography that could be downloaded by site users. In fact, the upload page on The Website clearly states: "Do not upload adult porn." Any user could create a free account on The Website by creating a username and password. Only after the user registered an account could the user browse previews of videos available for download and post text to The Website. To download videos from the site, users had to use "points," which were allocated to users by The Website. A registered user could earn points from The Website in several ways: (1) uploading videos depicting the sexual exploitation of children; (2) referring new users to The Website; (3) paying for a "VIP" account, which lasted for six months, entitled a user to unlimited downloads, and was priced at 0.03 Bitcoin (approximately \$327.60 USD as of March 1, 2018); or (4) paying for points incrementally.²

² Bitcoin ("BTC") is a type of virtual currency, circulated over the internet. BTC is not issued by any government, bank, or company, but rather is controlled through computer software operating via a decentralized, peer-to-peer network. BTC is just one of many varieties of virtual currency. To acquire BTC, a typical user purchases them from a BTC virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (e.g., U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and

As of February 8, 2018, The Website had over 125,000 unique videos available for downloading. In order to prevent duplicate videos from being uploaded, The Website provided a digital hash-value check in order for the user to compare his or her video to other videos previously uploaded to the site. The Website did not allow a user to upload a video whose hash value matched something previously uploaded to the site. According to law enforcement's viewing of The Website as of February 8, 2018, the videos stored on The Website amounted to over seven terabytes of data. As of February 8, 2018, The Website indicated on its download page details that its users had downloaded files from The Website more than one million times.

B. Defendant's Laundering of BTC to Promote Specified Unlawful Activity

Law enforcement identified the defendant's BTC account number, created on June 28, 2016 at a BTC exchange ("BTC Exchange"). In order to comply with due diligence obligations imposed by the BTC Exchange, the defendant provided his social security number, home address, phone number, driver's license number, and date of birth when opening his BTC Exchange account. The defendant linked his BTC Exchange account to two USAA Federal Savings bank debit cards in his name. On or about June 29, 2016, the defendant funded his BTC Exchange account via two transfers from his USAA Federal Savings account. Within a few minutes, the defendant sent a total of .06 BTC, via two transfers, to a wallet associated with The Website, which was in South Korea. The defendant only used his BTC Exchange account to fund his account at The Website.

virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities. It was through this "know your customer" policy that law enforcement were able to identify the defendant's BTC account number associated with payments to The Website.

Law enforcement's review of the forensic image of the electronic storage devices that had hosted The Website revealed that the defendant downloaded at least five videos from The Website. Two examples of these videos include the following:

- A video titled "Blogtv Smotri-2010-Glamour (12Yo Super Cute Girl Masturbate) Blackdress-Webcam.avi" with a description on The Website of "Cute WebcamGirl" – This video depicts a pre-pubescent female child wearing a black dress and exposes her vagina. She then rubs and insert her fingers into her vagina; and
- A video titled "mf16holland_omegle.mp4" with a description on The Website of "full sex omegle 13 years" – This video depicts a pre-pubescent male child and a pre-pubescent female child engaged in sexual activities with each other. The male child inserts his penis in the female child's mouth. Thereafter, the male child engages in vaginal intercourse with the female child.

C. Interview of Defendant

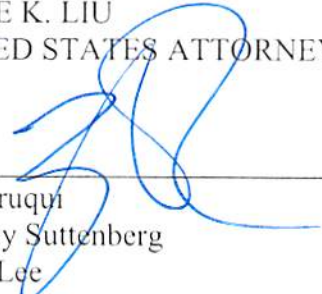
On August 9 2018, law enforcement conducted a non-custodial interview of the defendant. The defendant admitted to viewing child exploitation materials on the dark net via TOR, including on The Website, and the clear net since he was 12 years old. The defendant explained that he would use a Virtual Private Network service to anonymize accessing such sites. The defendant, who serves in the Air Force, stated that he accessed child exploitation materials while deployed with the Air Force the same way he does when he is at home. The defendant stated the last time he saw child exploitation materials was hours before the interview with law enforcement.

The defendant stated that he never retained any files; rather, he would download the videos and "shred it" afterwards, which he stated meant to securely erase the files. The defendant further explained that he never saved any such files for more than a few hours.

The defendant stated he sought counseling approximately two years ago from his pastor and from a trained medical professional. The defendant explained that he reached out for assistance because he knew that it was wrong to view child pornography.

Respectfully submitted,

JESSIE K. LIU
UNITED STATES ATTORNEY



Zia Faruqi
Lindsay Suttenger
Youli Lee
Assistant United States Attorneys

DEFENDANT'S ACKNOWLEDGMENT

I have read every page of this Statement of the Offense and have discussed it with my attorney. I fully understand this Statement of the Offense. I agree and acknowledge by my signature that this Statement of the Offense is true and accurate. I do this voluntarily and of my own free will. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this Statement of the Offense fully.

Date: 1/31/19


Brian James LaPrath
Defendant

ATTORNEY'S ACKNOWLEDGMENT

I have read every page of this Statement of the Offense, and have reviewed it with my client fully. I concur in my client's desire to adopt this Statement of the Offense as true and accurate.

Date: 1/31/19


David Benowitz
Defense Counsel